

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

TRAVIS CARTER,

Defendant.

Case No. 2:07-cr-00184-RLH-GWF

FINDINGS & RECOMMENDATIONS

Motion to Suppress Evidence - #25

This matter is before the Court on Defendant Travis Carter's Motion to Suppress Evidence (Franks Hearing Requested to Determine Whether the Application for the Search Warrant Was Misleading) (#25), filed on November 27, 2007 and the Government's Response to Defendant's Motion to Suppress Physical Evidence (#27), filed on November 29, 2007.

_____ Defendant Travis Carter is charged in a two count Indictment filed on August 15, 2007 with receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2) and possession of child pornography in violation of 18 U.S.C. § 2252A(5)(B). The Indictment arises out of evidence that the Government seized during the search of a residence on March 1, 2007 pursuant to a search warrant. Defendant alleges that the affidavit in support of the application for the search warrant contained material misstatements or omissions, absent which there would not have been probable cause to support the issuance of a search warrant. Defendant, therefore, requests that the Court conduct a *Franks* evidentiary hearing to determine whether the allegedly false statements or omissions in the affidavit were made intentionally or with reckless disregard for the truth. If the Court so concludes, then Defendant moves for suppression of the evidence.

FACTUAL BACKGROUND

The search warrant in this case was based on the affidavit of Sue A. Flaherty, a Special Agent (SA) with the Federal Bureau of Investigation (“FBI”). *Motion to Suppress* (#25), *Exhibit “A”*. Agent Flaherty’s affidavit contains a general discussion of the characteristics or behavior patterns of persons who produce, trade, distribute or possess images of minors engaged in sexually explicit conduct and how such persons use personal computers and the Internet to facilitate such activities. *Exhibit “A”*, Affidavit, pp. 3-6, ¶¶ 6-13. The affidavit also contains a Definitions section for key terms relating to child pornography and computer or Internet technology, *Id.*, pp. 6-8, ¶ 14, and a procedure for searching electronic data in computer hard drives and other memory storage devices. *Id.*, pp. 8-10, ¶¶ 15-18.

The specific factual information supporting the application for the search warrant was based on information provided to Agent Flaherty by Special Agent (SA) Wade Luders of the San Francisco Division of the FBI regarding his investigation of “the Ranchi message board.” On or about July 25, 2006, SA Luders became aware of the Ranchi message board which is a hard core child pornography message board located in Japan. SA Luders’ investigation of this message board over a six month period revealed that the only postings to it were sexually explicit videos and images (and related text) depicting children that constitute child pornography. *Exhibit “A”*, Affidavit, p. 11, ¶ 20. In order to access the Ranchi message board, Internet users were required to enter through a “gateway” or a website address that redirected the users to the current physical location of the message board. At any given time, there were three gateways to the Ranchi site most of which were located on web servers in Russia. *Id.*, ¶ 21. Upon entering the Ranchi message board, new users were directed to read the “FAQ” (Frequently Asked Questions) and “Tutorials” sections. These sections informed the user that the Ranchi message board contained a range of child pornography, including “hardcore baby material.” *Id.*, ¶¶ 21, 22. Other postings in these sections discussed how to encrypt and decrypt files, to remove identifying information from postings, to utilize online Internet tools to mask IP addresses, and generally how to evade law enforcement. *Id.*, ¶ 22. The Affidavit states that between July and December 2006, SA Luders downloaded multiple video and image files depicting children engaged in sexual acts with each other and with adults. *Id.*, p. 12, ¶ 24. The Affidavit contains specific written descriptions of some of the video files and image files downloaded by SA Luders which Agent Flaherty reviewed and

1 considered to constitute child pornography. *Id.*, p. 12, ¶¶ 24, 25.

2 The Affidavit states that because the Ranchi message board is hosted in Japan, whose child
3 pornography laws are different than those of the United States, SA Luders was unsuccessful in obtaining
4 a search warrant for user logs that would have enabled the Government to identify users who
5 downloaded from the links posted to the Ranchi message board. Consequently, SA Luders decided to
6 make undercover postings to the Ranchi message board that would capture the Internet Protocol (IP)
7 addresses of its users. SA Luders' postings to the Ranchi message board were consistent with other
8 postings he had observed there in that they advertised child pornography and contained hyperlinks that
9 purportedly connected to where child pornography could be downloaded. The hyperlinks created by SA
10 Luders actually connected to a covert FBI computer in San Jose, California, and the files contained
11 therein were encrypted and non-pornographic. The FBI computer captured the Internet Protocol (IP)
12 addresses of Ranchi message board users who attempted to download what was advertised as a child
13 pornography video. *Exhibit "A"*, p. 13, ¶ 27.

14 On October 25, 2006 at approximately 3:00 p.m Pacific Daylight Time (PDT), SA Luders, in an
15 undercover capacity, logged into the Ranchi message board and created a posting that advertised a video
16 of a four-year old female engaging in sexual activity with an adult male. The text of the posting read,
17 "here is one of my favs - 4yo hc with dad (toddler, some oral, some anal) -supercute! Haven't seen her
18 on the board before - if anyone has anymore, PLEASE POST." The posting directed individuals to go to
19 the certain website links (listed in the Affidavit) to download the video file. *Exhibit "A"*, p. 13, ¶ 28.

20 Approximately 40 minutes after the first posting, SA Luders posted another message on the
21 Ranchi message board, the purpose of which was to give the impression that he had accidentally posted
22 the wrong file to his previous posting. The text of SA Luders' second posting read, "sorry for the mixup
23 - I see I didn't post the right file I meant to (shit!) here is correct preview movie - others coming soon."
24 The second posting directed individuals to go to another website link in order to download the "correct"
25 video file. This link also returned to the covert FBI computer in San Jose, California which captured the
26 Internet Protocol (IP) addresses of the users who accessed the website link and attempted to download
27 the advertised video image. *Exhibit "A"*, pp. 13-14, ¶¶ 29, 30.

28 . . .

1 The Affidavit then sets forth Agent Flaherty's opinion that if someone attempted to download the
2 images posted by SA Luders, they would have done so intentionally and with full expectation that the
3 file contained child pornography. Agent Flaherty based her opinion on the content of SA Luders'
4 undercover postings and on the configuration and content of the Ranchi message board. *Exhibit "A"*, p.
5 14, ¶ 31. The Affidavit stated that there was probable cause to believe that prior to accessing SA
6 Luders' postings, the user would have had to know one of the gateways to access the Ranchi message
7 board, and would have been aware from the "FAQ" page that the message board contained illegal
8 material. Users would also have likely gone to the "FAQ" page to learn how to decrypt the downloaded
9 file which would have increased the users' awareness that the Ranchi message board contained illegal
10 materials. The Affidavit also noted that many other links on the Ranchi message board contained links
11 to child pornography. *Id.*

12 On October 26, 2006 at approximately 4:00 p.m. PDT, one day after his initial postings to the
13 Ranchi message board, SA Luders shut down the webserver on the covert FBI computer and copied and
14 preserved the log file which captured the Internet Protocol (IP) addresses that accessed the links he
15 posted on the Ranchi message board. *Exhibit "A"*, p. 15, ¶ 32. Several hundred unique IP addresses
16 attempted to download child pornography, i.e., the video image referred in SA Luders' posting. These
17 entries included five entries for Internet Protocol (IP) address 68.108.184.145. *Id.*, ¶ 33. The entries
18 associated with this IP address occurred between 7:12 p.m. and 7:15 p.m. PDT on October 25, 2006, and
19 between 1:19 a.m. and 1:27 a.m. PDT on October 26, 2006. *Id.*, ¶ 34.

20 The Affidavit then described the steps taken by the Government to identify the user of Internet
21 Protocol (IP) address 68.108.184.145. A search of the publicly available website arin.net revealed IP
22 address 68.108.184.145 was controlled by Cox Communications. On October 31, 2006, the Government
23 served an administrative subpoena on Cox Communications to identify the individual subscriber to IP
24 address 68.108.184.145 on October 25, 2006 at 7:12 p.m. PDT when a user of this IP address first
25 attempted to download the posting created by SA Luders on the Ranchi message board. On November
26 10, 2006, Cox Communications responded to the subpoena by identifying Luana Carter, 3815 North
27 Nellis Boulevard, Number 26, Las Vegas, Nevada 89115, telephone number 702-860-7293, as the
28 subscriber to IP address 68.108.184.145. *Exhibit "A"*, p. 16, ¶¶ 35-38. On January 17, 2007, the

1 Government conducted a search of the public records data base LexisNexis which indicted that Luana
2 Carter resided at the above listed address and that Defendant Travis Carter was a household member at
3 that address. *Id.*, ¶ 39. On January 17, 2007, the Government also checked Nevada Department of
4 Motor Vehicle (DMV) records which revealed a current driver's license for Luana Carter, with the same
5 social security number, date of birth and physical address obtained through LexisNexis. *Exhibit "A"*,
6 pp. 16-17, ¶ 40. On February 8, 2007, the Government also served an administrative subpoena on
7 Nevada Power Company for subscriber information for 3815 North Nellis Boulevard, Number 26, Las
8 Vegas, Nevada 89115. Nevada Power Company's response to the subpoena listed Luana Carter as
9 having an active account at that address since June 22, 2001 and listed her home telephone number as
10 702-860-7293. *Id.*, ¶ 41.

11 Agent Flaherty also stated that physical surveillance was conducted at 3815 North Nellis
12 Boulevard, Number 26, Las Vegas, Nevada on February 27, 2007 at which time she observed an Acura
13 automobile bearing Nevada license number 252-TPG parked in front of the mobile home residence at
14 that address. Nevada DMV records listed this vehicle as being registered to Defendant Travis Carter
15 with an address of 3815 North Nellis Boulevard, Number 26, Las Vegas, Nevada. *Exhibit "A"*, p. 17,
16 ¶42.

17 Based on the foregoing information, Agent Flaherty stated in her Affidavit that there was
18 "probable cause to believe that on October 25, 2006, someone using the Cox Communications Internet
19 account of Luana Carter attempted to violate Title 18, United States Code § 2252 and § 2252A by
20 attempting to download a file that was advertised as child pornography." *Exhibit "A"*, p. 17, ¶ 41[43].
21 Because the IP address returned to the Internet account of Luana Carter, whose address was 3815 North
22 Nellis Boulevard, Number 26, Las Vegas, Nevada, and there was still an active account in her name for
23 that address on the date of the Affidavit, Agent Flaherty also stated that she believed evidence of child
24 pornography crimes would be found at that residence. *Id.* Pursuant to the foregoing information, United
25 States Magistrate Judge Lawrence R. Leavitt issued a search warrant to search the premises at 3815
26 North Nellis Boulevard, Number 26, Las Vegas, Nevada, including computers and other data storage
27 devices for evidence of child pornography.

28 . . .

1 According to the Government's Response (#27), the search warrant was executed on March 1,
2 2007. Upon executing the warrant, the Government's agents learned that Defendant Travis Carter
3 resided at 3815 North Nellis Boulevard, Number 26, Las Vegas, Nevada with his mother Luana Carter
4 and his step-father. Defendant allegedly spoke with the agents and informed them that he had a
5 computer in his bedroom and was its only user. Defendant allegedly told the agents that when he was
6 not at home, he kept his bedroom door locked. Defendant also allegedly admitted to the agents that he
7 viewed images of child pornography on his computer and that he had visited the Ranchi site and had
8 downloaded images from that site. *Response* (#27), pp. 6-7. A subsequent forensic examination of
9 Defendant Carter's computer allegedly revealed thousands of child pornography images, including
10 videos or movies depicting child pornography. *Id.*, p. 7.

11 Defendant's Motion to Suppress Evidence (#25) challenges whether evidence that an Internet
12 Protocol (IP) address has allegedly been used to access and download child pornography, combined with
13 evidence regarding the IP address subscriber's identity and residential address, is sufficient to provide
14 probable cause to believe that evidence of child pornography will be found at the subscriber's residence.
15 Defendant argues that Agent Flaherty's Affidavit was misleading because it failed to inform the
16 Magistrate Judge of material facts regarding Internet access through an Internet services provider such as
17 Cox Communications and how IP addresses function. Defendant argues that if such information had
18 been included in the affidavit, probable cause would have been lacking. In support of his motion,
19 Defendant has submitted (1) an affidavit of Adrian Leon Mare, an expert in computer networking,
20 computer forensics, electronic evidence discovery and electronic data recovery, *Exhibit "D"*; (2) an
21 affidavit by Al Tobin, an investigator with the Federal Public Defender, District of Nevada, *Exhibit "B"*;
22 and (3) an aerial or satellite photograph of the location of Defendant's residence, *Exhibit "C"*.
23 Defendant has also referred the Court to a November 10, 2004 article on the FBI's website entitled
24 "Internet Security in a Wireless World, The Case of the Not-So-Friendly Neighborhood Spammer." *See*
25 *Defendant's Motion* (#25), p. 12.

26 The affidavit of Defendant's expert witness, Adrian Mare, states that he has worked in various
27 positions in the computer industry for over 25 years, that he has been certified as a systems engineer or
28 specialist by leading computer companies, such as Microsoft and Cisco Systems, and that he has been

1 trained in advanced Internet forensics. *Motion* (#25), *Exhibit "D"*, ¶ 1. Mr. Mare's affidavit makes the
2 following points:

- 3 * Computers access the Internet through connections or portals. Each of these portals or
4 connections is assigned its own Internet Protocol (IP) address. Each time a computer
5 accesses the Internet, it is assigned an IP address. ¶ 4.
- 6 * One way a computer user can gain access to an IP address is to become a subscriber to an
7 Internet Service Provider (ISP), such as Cox Communications. Cox Communications
8 provides Internet service in portions of Las Vegas. It is not necessary or required by ISPs
9 such as Cox for the ISP to actually go to a location to establish Internet service for a
10 client. A client can establish an Internet account without having an ISP come to a
11 particular location to establish service. ¶ 5.
- 12 * Upon becoming a subscriber, the computer user is permitted to connect to the
13 ISP's network by physically attaching a connecting device, a cable modem, to
14 cables located in his/her residence or business. A cable modem can only be
15 physically connected to cables in a house, building or structure if cables are
16 physically present in the structure, and not all buildings or structures have such
17 wiring or cables. ¶ 6
- 18 * In order to allow multiple computers to access the Internet under the same IP address, the
19 cable modem may be connected to a router, or may itself function as a router, which
20 serves as a gateway through which multiple computers could access the Internet at the
21 same time under the same IP address. The router could be a wireless device in which case
22 computers located within 300 feet of the wireless router signal could access the Internet
23 through the router and modem under the same IP address. The wireless router signal
24 strength could be increased beyond 600 feet if additional devices are added. The only
25 way to prevent sharing of the wireless router is to encrypt the signal and even then an
26 individual can bypass this security using publicly available software. ¶¶ 7-8.
- 27 * Each time a computer accesses the Internet through a router it is assigned an IP
28 address. The IP address is actually assigned to the cable modem or router.
Therefore, every computer which accesses the Internet through the same router
will have the same IP address. Computers may also access the Internet without a
router through another computer, which process is known as "Internet connection
sharing." ¶¶ 9-10.
- * Computers can be in various locations while still simultaneously accessing the
same wireless router. All computers accessing the Internet through the same
wireless router will have the same IP address. ¶ 12.
- * Each piece of computer hardware, i.e, modem, router or computer has a unique
media access control (MAC) number or address. The MAC address is assigned
by the manufacturer when the device is created. Each device, even if it the same
type and model, will have a unique MAC address. When pieces of hardware are
connected, they can communicate their MAC addresses to each other. ¶ 13.
- * There is publicly available software on the Internet which permits a computer to "spoof"
or fake an IP address in another network. Through this software an individual can make
it appear that he is using a specific router when he is, in fact, using a different router.
Thus, when this person sends a message or information to another computer, the
receiving computer will be unaware of the true IP address of the sending computer. ¶ 14.

1 * There is also publicly available software which permits a computer to “spoof” or fake the
2 media access control (MAC) number or address of the computer, modem or router, which
3 would prevent the ISP, such as Cox Communication, from knowing who is actually using
 its network to access the Internet. ¶ 15.

4 Mr. Mare further states that based on his professional experience in Las Vegas, he knows that
5 there are communities and neighborhoods in Las Vegas which have created their own network by
6 sharing one Internet connection and thus one IP address between several households. *Motion* (#25),
7 *Exhibit “D”*, ¶ 16. Based on the foregoing, Mr. Mare states that there are many problems with using an
8 IP address to decide the location of a computer allegedly using an IP address on the Internet. The IP
9 address can be “spoofed.” A single IP address can be used by multiple computers at multiple locations
10 through a wireless router. The MAC address of a cable modem can be spoofed to allow access to
11 another’s Internet connection. A neighborhood with several houses can share one Internet connection
12 and therefore have the same IP address. *Id.*, ¶ 17.

13 According to the affidavit of the Federal Public Defender’s investigator, Al Tobin, he
14 interviewed a former employee of Cox Communications, April Lindskog, by telephone on September
15 28, 2007. Ms. Lindskog indicated in that interview that to her knowledge, Cox Communications tracks
16 its subscribers’ usage based on the MAC number or address of the cable modem associated with the
17 account. Ms. Lindskog explained that a cable modem registered for an account could connect to Cox
18 anywhere that Cox provided service and that a customer’s access to Cox was not limited by geographical
19 location or address. *Motion* (#25), *Exhibit “B”*, ¶¶ 3-5. Mr. Tobin also stated that he visited the vicinity
20 of 3815 North Nellis Boulevard, Number 26, Las Vegas, Nevada, and based on his preliminary
21 investigation, there are over 200 homes located within approximately 600 feet of Defendant’s residence.
22 *Id.* ¶ 6.

23 The Court has also reviewed the FBI article, “Internet Security in a Wireless World, The Case of
24 the Not-So-Friendly Neighborhood Spammer,” referenced in Defendant’s Motion. The article states that
25 there are people who drive around neighborhoods and office parks with laptop computers looking for
26 open or unprotected wireless access points to the Internet. These persons electronically hijack the web
27 connections they find and use them to send unsolicited spam. Such persons can use the person’s Internet
28 connection and IP address to send spam to other computers, including child pornography. The article

1 also discusses steps that a computer user can take to protect his or her wireless device from being
2 hijacked.

3 DISCUSSION

4 As both parties note in their respective briefs, this Court previously issued findings and
5 recommendations in *United States v. Latham*, Case No. 2:06-cr-379-LDG (GWF) (hereinafter
6 “*Latham*”) which involved a substantially similar motion to suppress and request for a *Franks* hearing.
7 The motion in *Latham* was also supported by affidavits by Defendant’s computer expert, Adrian Mare,
8 and by investigator Al Tobin which contain substantially the same information set forth in their
9 affidavits in support of Defendant Carter’s instant motion. *See Latham Motion to Suppress* (#50). The
10 undersigned Magistrate Judge recommended that Defendant Latham’s motion to suppress and request
11 for a *Franks* hearing be denied. *See Latham Report and Recommendations* (#56). District Judge George
12 adopted the Report and Recommendations and denied Defendant Latham’s motion to suppress. *See*
13 *Latham Order* (#70).

14 The affidavit of Mr. Mare in support of Defendant Carter’s instant motion contains some
15 additional information that was not included in his affidavit in *Latham*. In particular, the information set
16 forth in paragraph 16, regarding local neighborhood networks, and Mr. Mare’s opinions in paragraph 17
17 were not included in his earlier affidavit. Otherwise, the information in both affidavits is substantially
18 the same. The FBI website article was not provided in the motion in *Latham*. With this additional
19 information also in mind, the Court proceeds with a discussion and evaluation of Defendant Carter’s
20 instant motion.

21 In *Franks v. Delaware*, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), the Supreme Court
22 held that the Fourth Amendment entitles a defendant to challenge the validity of a search warrant
23 affidavit if the defendant makes a substantial preliminary showing that (1) the affidavit contains
24 intentionally or recklessly false statements and (2) the affidavit purged of its falsities would not be
25 sufficient to support a finding of probable cause. *See United States v. Martinez-Garcia*, 397 F.3d 1205,
26 1215 (9th Cir. 2005), *citing United States v. Reeves*, 210 F.3d 1041, 1044 (9th Cir. 2000). In making the
27 initial determination of whether a defendant is entitled to an evidentiary hearing, *Franks* states:

28 . . .

There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient.

438 U.S. at 171.

Franks further stated that if the defendant makes a substantial showing that the affidavit contains intentionally or recklessly false statements, "and if, when the material that is the subject of the alleged falsity is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Id.*, at 171-172. On the other hand, if the remaining content is insufficient to support probable cause, then the defendant is entitled to an evidentiary hearing. *Id.* At such hearing, the defendant has the burden of proof by a preponderance of the evidence to establish that the false statements were deliberately made or were made with a reckless disregard for the truth. *United States v. DeLeon*, 955 F.2d 1346, 1348 (9th Cir. 1992).

As the Ninth Circuit recently reiterated in *United States v. Jawara*, 474 F.3d 565, 582 (9th Cir. 2007), intentional or reckless omissions may also provide grounds for a *Franks* hearing. The Court stated:

"A search warrant, to be valid, must be supported by an affidavit establishing probable cause." *United States v. Stanert*, 762 F.2d 775, 778 (9th Cir.1985). In *Stanert*, we applied the rationale of *Franks v. Delaware*, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), to hold that a defendant could challenge a facially valid affidavit by making a substantial preliminary showing that "the affiant intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading." *Stanert*, 762 F.2d at 781 ("By reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw. To allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real meaning.") In addition, the defendant must show that the "affidavit, once corrected and supplemented," would not "provide ... a substantial basis for concluding that probable cause existed" to search defendant's residence. *Id.* at 782.

Stanert also states that in determining whether a defendant is entitled to an evidentiary hearing, "[c]lear proof of deliberate or reckless omission is not required. See *United States v. Chesner*, 678 F.2d

1 1353, 1362 (9th Cir. 1982). Such proof is reserved for the evidentiary hearing.” 762 F.2d at 781. The
2 search warrant affidavit in *Stanert* alleged that defendant’s residence was being used as an illegal drug
3 laboratory. The court found that defendant had made a substantial preliminary showing that the affidavit
4 omitted material information regarding each of the key facts relied on by the government to support
5 probable cause and that the nature of the omissions suggested that they were made intentionally or at
6 least recklessly. Probably the most glaring example was the affiant’s statement that an illicit drug lab
7 had previously exploded at the residence. The affidavit did not inform the issuing judge, however, that
8 defendant did not purchase or move into the residence until after that explosion. The court also held that
9 if the omitted information had been included in the affidavit, there would not have been a substantial
10 basis upon which to find probable cause. Defendant was therefore entitled to a *Franks* hearing to
11 determine whether the officer’s omissions were intended to deceive the issuing judge or were made with
12 reckless disregard for the truth.

13 As *Stanert* indicates, the materiality of the omitted information in regard to probable cause is
14 relevant to the defendant’s initial preliminary showing that the omissions were made intentionally or
15 recklessly. The Seventh Circuit has stated that Defendant “must offer direct evidence of the affiant’s
16 state of mind or inferential evidence that the affiant had obvious reasons for omitting facts in order to
17 prove deliberate falsehood or reckless disregard.” *United States v. Souffront*, 338 F.3d 809, 822-23 (7th
18 Cir. 2003). In this latter regard, the nature of the omitted facts must be such that it is reasonable to infer
19 that they were deliberately or intentionally omitted from the affidavit. *See e.g. Stanert, supra*, (advising
20 judge about previous drug lab explosion, but failing to disclose that it occurred before the defendant
21 owned or resided on the premises indicated at least a reckless disregard for the truth.)

22 The affidavit in this case provides a fairly detailed description of the means and methods by
23 which persons use computers and the Internet to exchange and download images of child pornography.
24 *See Motion (#25), Exhibit “A”, Affidavit*, pp. 3-6. As this Court stated in *Latham* and reiterates here, it
25 is reasonable to infer that the FBI agents who prepared or assisted in preparing the search warrant
26 affidavit understand how IP addresses function and the extent to which IP addresses indicate where a
27 particular computer is located. The issue before the Court, therefore, is whether the alleged omissions
28 here would have defeated probable cause had they been included in the affidavit and, if so, whether they

1 sufficiently evidence deliberate falsehood or reckless disregard for the truth to warrant a *Franks*
2 evidentiary hearing.

3 In *United States v. Kelley*, 482 F.3d 1047, 1050-51 (9th Cir. 2007), the Ninth Circuit recently
4 reiterated the standards for determining probable cause as spelled out in *Illinois v. Gates*, 462 U.S. 213,
5 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). The court noted that these standards apply with equal force to
6 cases involving child pornography on a computer. *United States v. Gourde*, 440 F.3d 1065, 1069 (9th
7 Cir. 2006) (en banc). *Kelley* states:

8 Thus, probable cause means a “fair probability” that contraband or
9 evidence is located in a particular place. *Gates* 462 U.S. at 246, 103 S.Ct.
10 2317; *Gourde*, 440 F.3d at 1069. Whether there is a fair probability
11 depends upon the totality of the circumstances, including reasonable
12 inferences, and is a “commonsense, practical question.” *Gourde*, 440 F.3d
13 at 1069 (citing and quoting *Gates*, 462 U.S. at 230, 246, 103 S.Ct. 2317).
14 Neither certainty nor a preponderance of the evidence is required. *Id.*
15 (citing *Gates*, 462 U.S. at 246, 103 S.Ct. 2317).

16 Normally, we do not “flyspeck” the affidavit supporting a search warrant
17 through de novo review; rather, the magistrate judge’s determination
18 “should be paid great deference.” *Gourde*, 440 F.3d at 1069 (quoting
19 *Gates*, 462 U.S. at 236, 103 S.Ct. 2317 (quoting *Spinelli v. United States*,
20 393 U.S. 410, 419, 89 S.Ct. 584, 21 L.Ed.2d 637 (1969))). In addition, the
21 Supreme Court has reminded reviewing courts that “[a]lthough in a
22 particular case it may not be easy to determine when an affidavit
23 demonstrates the existence of probable cause, resolution of doubtful or
24 marginal cases in this area should largely be determined by the preference
25 to be accorded to warrants.” *Gates*, 462 U.S. at 237 n. 10, 103 S.Ct. 2317
26 (quoting *United States v. Ventresca*, 380 U.S. 102, 109, 85 S.Ct. 741, 13
27 L.Ed.2d 684 (1965)).

19 In *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir.2006) (en banc), the government
20 obtained a warrant to search defendant’s residence and personal computer for child pornography based
21 on information in the affidavit that defendant had subscribed to and remained a member of an Internet
22 website which charged a monthly fee, and which advertised and allowed members to view and download
23 both legal pornography and illegal child pornography. The affidavit also discussed the characteristics of
24 persons who collect child pornography, including their general habits in retaining child pornography on
25 their computers or elsewhere in their residences. The *en banc* majority held that the affidavit provided a
26 fair probability that defendant had downloaded child pornography from the website and retained it in his
27 possession at the time the warrant was issued. The majority therefore held that the search warrant was
28 supported by probable cause. Relying on *Gourde*, the court in *Kelley* similarly held that the

1 government's affidavit provided sufficient evidence for probable cause to believe that defendant had
2 knowingly received and possessed email communications with attachments containing child
3 pornography images.

4 Defendant Carter does not dispute that Agent Flaherty's affidavit provided probable cause to
5 believe that the person(s) who accessed the links on the posting that SA Luders created on the Ranchi
6 website through IP address 68.108.184.145 did so intentionally and with knowledge that he or she was
7 attempting to access illegal child pornographic images. Defendant argues, however, that the affidavit
8 was misleading in representing or suggesting that the identification of the name and address of the
9 subscriber for IP address 68.108.184.145 was sufficient to establish probable cause to believe that the
10 person using that IP address on October 25-26, 2006 was located on the premises at 3815 North Nellis
11 Boulevard, Number 26, Las Vegas, Nevada, and that evidence of illegal child pornography would be
12 found on those premises. Defendant argues that the Government knew or should have known of the
13 other possibilities set forth in Mr. Mare's affidavit regarding the use of IP address 68.108.184.145
14 which, if included in the affidavit, would have negated probable cause regarding the location of the
15 evidence.

16 The Fifth Circuit in *United States v. Perez*, 484 F.3d 735 (5th Cir. 2007), rejected a similar
17 argument as sufficient to defeat probable cause. In *Perez*, a woman complained to the police that
18 someone with the Yahoo ID "famcple" sent her an Internet message containing child pornography. The
19 police forwarded the complaint to the FBI. Through a subpoena to Yahoo!, Inc., the FBI determined that
20 on the dates the child pornography was transmitted, the computer used IP address 24.27.21.6. The FBI
21 determined that this IP address was owned by Time Warner Cable and, through a subpoena to Time
22 Warner, learned that the IP address was assigned to defendant. Based on this information, the FBI
23 obtained a search warrant to search defendant's residence. Defendant argued that the "mere association
24 between an IP address and physical address is insufficient to establish probable cause." In rejecting this
25 argument, the Court stated:

26 In this case it is clear that there was a substantial basis to conclude that
27 evidence of criminal activity would be found at 7608 Scenic Brook Drive.
28 The affidavit presented to the magistrate included the information that the
child pornography viewed by the witness in New York had been
transmitted over the IP address 24.27.21.6, and that this IP address was

1 assigned to Javier Perez, residing at 7608 Scenic Brook Drive, Austin,
2 Texas 78736. Perez argues that the association of an IP address with a
3 physical address does not give rise to probable cause to search that
4 address. He argues that if he “used an unsecure wireless connection, then
5 neighbors would have been able to easily use [Perez’s] internet access to
6 make the transmissions.” But though it was possible that the
7 transmissions originated outside of the residence to which the IP address
8 was assigned, it remained likely that the source of the transmissions was
9 inside that residence. *See United States v. Grant*, 218 F.3d 72, 73 (1st
10 Cir. 2000) (stating that “even discounting for the possibility that an
11 individual other than [defendant] may have been using his account, there
12 was a *fair probability* that [defendant] was the user and that evidence of
13 the user’s illegal activities would be found in [defendant’s] home”)
14 (emphasis in original). “[P]robable cause does not require proof beyond a
15 reasonable doubt.” *Brown*, 941 F.2d at 1302.

16 Perez also argues that evidence that illicit transmissions were made does
17 not give rise to probable cause that physical evidence would be located at
18 the residence. However, the New York witness stated that the images she
19 observed appeared to be videos played on a television screen transmitted
20 via a web cam. There was therefore a basis to believe that the suspect
21 would have such videos in his residence. Moreover, Britt stated in his
22 affidavit that, in his experience, persons interested in child pornography
23 typically retain numerous images of child pornography as well as “material
24 documenting the arrangements, the introduction, and tasks to consummate
25 the acquisition of child pornography.” Based on this information, there
26 was probable cause to believe that physical evidence of violations of the
27 child pornography laws would be located at 7608 Scenic Brook Drive.

28 *Perez*, 484 F.3d at 740-41.

1 In deciding whether the Defendant has made a sufficient threshold showing to warrant a *Franks*
2 evidentiary hearing, the Court assumes that the factual information set forth in Mr. Mare’s and Mr.
3 Tobin’s affidavits is accurate. The article on the FBI website also verifies that an outsider can use a
4 subscriber’s wireless connection and IP address to gain access to the Internet and, among other things,
5 use that connection and IP address to either send or receive child pornography. The fact that an outside
6 computer user can gain access to the Internet through the Internet service subscriber’s wireless
7 connection and IP address, with or without his knowledge, or that computer users can use software to
8 “spoof” another person’s assigned IP address or MAC address, are certainly possibilities that diminish
9 the likelihood that the Internet transmission emanated from the subscriber’s premises.

10 The Court nevertheless agrees with *Perez* that even if the information set forth in Mr. Mare’s
11 and Mr. Tobin’s affidavits had been included in Agent Flaherty’s affidavit, there would still have
12 remained a likelihood or *fair probability* that the transmission emanated from the subscriber’s place of

1 residence and that evidence of child pornography would be found at that location. The Defendant,
2 therefore, has not met his initial burden to show “that the ‘affidavit, once corrected and supplemented,’
3 would not ‘provide ... a substantial basis for concluding that probable cause existed’ to search
4 defendant's residence.” *United States v. Jawara*, 474 F.3d at 582, *quoting Stanert*. Additionally, unlike
5 the circumstances in *Stanert, supra*, where the omitted information would have clearly negated probable
6 cause, the omissions in this case do not support an inference that they were made intentionally to mislead
7 the Court or with reckless disregard for the truth.

8 CONCLUSION

9 The Court concludes that Defendant has not made the threshold showing to warrant a *Franks*
10 evidentiary hearing because the omitted information, if included in the affidavit, would not have negated
11 a substantial basis for concluding that there was probable cause to believe that evidence of child
12 pornography would be found on the premises to be searched. Given this conclusion, there are also no
13 grounds to support an inference that the omissions were intentional or made with reckless disregard for
14 the truth. Accordingly,

15 RECOMMENDATION


16 **IT IS RECOMMENDED** that Defendant’s Motion to Suppress Evidence (Franks Hearing
17 Requested to Determine Whether the Application for the Search Warrant Was Misleading) (#25) be
18 **denied**.

19 NOTICE

20 Pursuant to Local Rule IB 3-2, any objection to this Finding and Recommendation must be in
21 writing and filed with the Clerk of the Court within ten (10) days. The Supreme Court has held that the
22 courts of appeal may determine that an appeal has been waived due to the failure to file objections within
23 the specified time. *Thomas v. Arn*, 474 U.S. 140, 142 (1985). This circuit has also held that (1) failure
24 to file objections within the specified time and (2) failure to properly address and brief the objectionable
25 issues waives the right to appeal the District Court’s order and/or appeal factual issues from the order of
26 ...
27 ...
28 ...

1 the District Court. *Martinez v. Ylst*, 951 F.2d 1153, 1157 (9th Cir. 1991); *Britt v. Simi Valley United*
2 *Sch. Dist.*, 708 F.2d 452, 454 (9th Cir. 1983).

3 DATED this 7th day of February, 2008.

4 
5 GEORGE FOLEY, JR.
6 United States Magistrate Judge
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28